

Article - State Government

[\[Previous\]](#)[\[Next\]](#)

§18–223.

(a) (1) Unless the Secretary of State adopts an applicable and superseding regulation under § 18–222 of this subtitle in the manner provided in this subsection, a notary public shall comply with the requirements of this section when performing a notarial act with respect to an electronic record or a remotely located individual.

(2) A regulation adopted by the Secretary of State may supersede a requirement of this section if the regulation references this section and specifies the requirement to be superseded.

(b) When necessary under § 18–214(a)(1)(iii) of this subtitle, identity proofing and credential analysis shall be performed by a reputable third party who has provided evidence to the notary public of the ability to satisfy the requirements of this section.

(c) When necessary under § 18–214(a)(1)(iii) of this subtitle, identity proofing shall be performed through a dynamic knowledge–based authentication that meets the following requirements:

(1) each remotely located individual must answer a quiz consisting of a minimum of five questions related to the individual’s personal history or identity, formulated from public or private data sources;

(2) each question must have a minimum of five possible answer choices;

(3) at least 80% of the questions must be answered correctly;

(4) all questions must be answered within 2 minutes;

(5) if the remotely located individual fails the first attempt, the individual may retake the quiz one time within 24 hours;

(6) during a retake of the quiz, a minimum of 40% of the prior questions must be replaced;

(7) if the remotely located individual fails the second attempt, the individual is not allowed to retry with the same notary public within 24 hours of the second failed attempt; and

(8) the notary public must not be able to see or record the questions or answers.

(d) When necessary under § 18–214(a)(1)(iii) of this subtitle, credential analysis must use public or private data sources to confirm the validity of an identification credential presented by a remotely located individual and shall, at a minimum:

(1) use automated software processes to aid the notary public in verifying the identity of each remotely located individual;

(2) ensure that the identification credential passes an authenticity test, consistent with sound commercial practices that:

(i) use appropriate technologies to confirm the integrity of visual, physical, or cryptographic security features;

(ii) use appropriate technologies to confirm that the identification credential is not fraudulent or inappropriately modified;

(iii) use information held or published by the issuing source or an authoritative source, as available, to confirm the validity of personal details and identification credential details; and

(iv) provide output of the authenticity test to the notary public;
and

(3) enable the notary public visually to compare for consistency the information and photo on the identification credential and the remotely located individual as viewed by the notary public in real time through communication technology.

(e) (1) Communication technology shall provide reasonable security measures to prevent unauthorized access to:

(i) the live transmission of the audio–visual feeds;

(ii) the methods used to perform credential analysis and identity proofing, if credential analysis and identity proofing are necessary under § 18–214(a)(1)(iii) of this subtitle; and

(iii) the electronic record that is the subject of the notarial act, if there is an electronic record instead of a tangible record.

(2) If a remotely located individual must exit the workflow, the remotely located individual must meet the criteria of this section and restart credential analysis and identity proofing from the beginning.

(f) (1) If the notarial act is regarding an electronic record, a notary public shall attach or logically associate the notary public's electronic signature and official stamp to an electronic record by use of a digital certificate complying with the X.509 standard adopted by the International Telecommunication Union or a similar industry-standard technology.

(2) If the notarial act is regarding a tangible record, § 18–215(b)(1) of this subtitle applies.

(3) A notary public may not perform a notarial act with respect to an electronic record if the digital certificate:

- (i) has expired;
- (ii) has been revoked or terminated by the issuing or registering authority;
- (iii) is invalid; or
- (iv) is incapable of authentication.

(g) (1) A notary public shall retain a journal required under § 18–219 of this subtitle and any audio–visual recordings required under § 18–214 of this subtitle in a computer or other electronic storage device that protects the journal or audio–visual recordings against unauthorized access by password or cryptographic process.

(2) (i) A notary public may, by written contract, engage a third party to act as a repository to provide the storage required by paragraph (1) of this subsection.

(ii) The contract shall:

1. enable the notary public to comply with the retention requirements of this subtitle even if the contract is terminated; or

2. provide that the information will be transferred to the notary public if the contract is terminated.

(3) A third party under contract with a notary public under this subsection shall be deemed a repository approved by the Secretary of State under § 18–219 of this subtitle.

[\[Previous\]](#)[\[Next\]](#)